

## Obsah

|          |  |           |
|----------|--|-----------|
| <b>1</b> | <b>Všeobecné údaje stavby .....</b>                              | <b>2</b>  |
| 1.1      | Identifikace stavby .....  | 2         |
| 1.2      | Zadavatel projektové dokumentace .....                           | 2         |
| 1.2.1    | Objednatel (investor) .....                                      | 2         |
| 1.2.2    | Zhotovitel projektové dokumentace stavby .....                   | 2         |
| <b>2</b> | <b>Stávající stav .....</b>                                      | <b>3</b>  |
| 2.1      | Segmentace provozu .....   | 3         |
| 2.2      | Přenosový systém DWDM, IP/MPLS .....                             | 3         |
| <b>3</b> | <b>Související nebo navazujících investiční akce.....</b>        | <b>4</b>  |
| <b>4</b> | <b>Základní charakteristika segmentace a jejího užívání.....</b> | <b>5</b>  |
| 4.1      | Základní technické řešení .....                                  | 5         |
| 4.2      | Rozsah segmentace provozu v TDS .....                            | 5         |
| 4.3      | Koncepce technického řešení v navrhované stavbě.....             | 5         |
| 4.3.1    | Segmentace provozu v technologické datové síti.....              | 5         |
| 4.3.2    | Podpora subsystémů kybernetické bezpečnosti.....                 | 6         |
| <b>5</b> | <b>Návrh technického řešení.....</b>                             | <b>8</b>  |
| 5.1      | Segmenty .....   | 8         |
| 5.2      | Škálovatelnost segmentace .....                                  | 10        |
| 5.3      | Architektura segmentace .....                                    | 11        |
| 5.4      | Řízení prostupů na FW .....                                      | 11        |
| 5.5      | Komunikační pravidla, matice .....                               | 14        |
| 5.6      | Dimenzování firewallů.....                                       | 15        |
| 5.7      | PS 3-101 OŘ Praha, segmentace provozu.....                       | 15        |
| 5.8      | PS 3-102 OŘ Plzeň, segmentace provozu.....                       | 15        |
| 5.9      | PS 3-103 OŘ Ústí nad Labem, segmentace provozu .....             | 15        |
| 5.10     | PS 3-104 OŘ Hradec Králové, segmentace provozu .....             | 15        |
| 5.11     | PS 3-105 OŘ Brno, segmentace provozu.....                        | 15        |
| 5.12     | PS 3-106 OŘ Olomouc, segmentace provozu .....                    | 15        |
| 5.13     | PS 3-107 OŘ Ostrava, segmentace provozu .....                    | 15        |
| 5.13.1   | Umístění zařízení .....  | 16        |
| 5.14     | PS 3-108 Předimplementační analýza a centrální části.....        | 17        |
| <b>6</b> | <b>Ochrana elektrických rozvodů .....</b>                        | <b>19</b> |
| 6.1      | Prostředí.....   | 19        |
| 6.2      | Ochrana před nebezpečným dotykem živých částí.....               | 19        |
| 6.3      | Ochrana před nebezpečným dotykem neživých částí.....             | 19        |
| <b>7</b> | <b>Životní prostředí, likvidace odpadů .....</b>                 | <b>20</b> |
| <b>8</b> | <b>Bezpečnost a ochrana zdraví při práci .....</b>               | <b>21</b> |
| <b>9</b> | <b>Pokyny pro montáž a demontáž.....</b>                         | <b>22</b> |
| 9.1      | Požadavky na zabezpečení provozu a realizace.....                | 22        |
| 9.2      | Péče o životní prostředí.....                                    | 22        |

# 1 Všeobecné údaje stavby

## 1.1 Identifikace stavby

|                                     |  |
|-------------------------------------|--|
| <b>Název stavby:</b>                | Segmentace provozu v technologické datové síti                                 |
| <b>Stupeň dokumentace:</b>          | Dokumentace pro územní řízení  |
| <b>Druh/Charakter stavby:</b>       | Stavba dráhy/ Technologická stavba železniční infrastruktury                   |
| <b>Cíl stavby:</b>                  | Segmentace provozu v technologické datové síti pomocí VRF/VPN                  |
| <b>Kraj:</b>                        | Praha, Ústecký, Plzeňský, Pardubický, Jihomoravský, Moravskoslezský, Olomoucký |
| <b>Vlastníci dotčených pozemků:</b> | Správa železnic, státní organizace (ostatní viz geodetická část PD)            |
| <b>Místo stavby:</b>                | Praha, Plzeň, Ústí nad Labem, Pardubice, Brno, Ostrava, Olomouc                |
| <b>Dodavatel:</b>                   | Bude určen na základě výběrového řízení  |
| <b>Hlavní inženýr projektu:</b>     | Ing. Martin Štrof<br>(martin.strof@sudop.cz, tel. 267 094 144, 605 229 014)    |

## 1.2 Zadavatel projektové dokumentace

### 1.2.1 Objednatel (investor)

|                    |   |
|--------------------|---|
| <b>Investor:</b>   | <b>Správa železnic, státní organizace</b><br><b>Dlážděná 1003/7, 110 00 Praha 1</b><br>IČ: 70994234, DIČ: CZ70994234<br>Zapsaná v OR vedeném u Městského soudu v Praze, oddíl A, vložka 48384 |
| <b>Zastoupený:</b> | <b>Správa železnic, státní organizace</b><br><b>Stavební správa západ</b><br>Sokolovská 278/1955, 190 00 Praha 9  |

### 1.2.2 Zhotovitel projektové dokumentace stavby

|                     |   |
|---------------------|---|
| <b>Zpracovatel:</b> | SUDOP PRAHA a.s.<br>208 Středisko elektrotechniky, trakce, sdělovací a zabezpečovací techniky<br>Olšanská 1a, 130 80 Praha 3<br>IČ: 257 93 349, DIČ: CZ 257 93 349<br>Zapsaný v OR u Městského soudu v Praze, oddíl B, č. vložky 6088 |
|---------------------|---|

## 2 Stávající stav

### 2.1 Segmentace provozu

Různorodost požadavků uživatelů aplikací a správců systému i navazujících procesů uživatele vyžaduje výkonné prostředky pro segmentaci sítě jako základní prostředek řízení informačních toků.

V současné době existují v přenosové síti Správy železnic desítky decentralních prostupů do jiných sítí, která mají nastavena individuální pravidla komunikace. V některých případech existují i dial-up přístupy k technologiím od dodavatelů. Do přenosové sítě Správy železnic mají přístup i externí subjekty (např. ČD, ČD Cargo, ČD IS a další) za účelem správy údržby nasazených zařízení a aplikací. V dalších krocích rozvoje přenosové sítě a také s ohledem na zákon č. 181/2014 Sb., o kybernetické bezpečnosti je nutné provést vyčlenění externích subjektů do samostatné oddělené sítě s řízeným prostupem, umístěním za Firewall do přidělené VPN.

### 2.2 Přenosový systém DWDM, IP/MPLS

V současné době jsou přenosové sítě Správy železnic tvořeny dvěma hlavními systémy. Starší systém budovaný v souvislosti s modernizacemi a optimalizacemi tratí je systém SDH (synchronní digitální hierarchie). Datová síť historicky vybudovaná pomocí modemů provozovaných po stávajících dálkových kabelech a s příchodem optických vláken postupně přebudovávaná na propojování datových prvků pomocí optických převodníků, a to IMC modemů a v poslední řadě pomocí SFP převodníků, které jsou součástí datových přepínačů. Jednotlivé uzly přenosové sítě SDH jsou vystavěny s použitím technologie Cisco ONS 15305 a uzly pro překryvnou síť s rychlostí STM-16 jsou vystavěny z boxů ONS 15454. Přenosové rychlosti v síti SDH jsou STM-1 (menší ŽST., BTS systému GSM-R, některé energetické objekty), STM-4 (většina železničních stanic) a STM-16 (překryvná úroveň přenosové sítě). Firma Cisco ukončila dodávky uvedené technologie ONS 15305 do ČR, pokračuje se ještě s výstavbou větších přenosových uzlů ONS 15454 v rámci překryvné sítě. V případě dodržení jednotného přenosového traktu se výjimečně nově dobudované SDH používají boxy od společnosti Ericsson, a to typy SPO 1410 používané jako náhrada ONS 15305 a SPO 1460 jako náhrada boxu ONS 15454. Pro nově připravované stavby se již uvažuje s přenosovou technologií synchronního Ethernetu s IP/MPLS protokolem.

V roce 2015 byla vybudována nová přenosová síť realizovaná přenosovým systémem DWDM (Dense Wavelength Division Multiplexing) od společnosti Cisco typem Cisco NCS2000, který byl umístěn v 11 lokalitách uzlových stanic (v některých i více šasí) a dalšími body, ve kterých byly instalovány nezbytné opakovače DWDM (celkem 10 lokalit) z důvodu nevyhovujícího útlumu přenosové cesty vzhledem k velké vzdálenosti.

Zároveň s výstavbou přenosové sítě DWDM byly rovněž vybudovány v obou CDP Praha i CDP Přerov nové Core routery MPLS (P) postavené na technologii Cisco ASR 9912, které zabezpečují přechod mezi oběma úrovněmi přenosů, tedy mezi úrovní super páteře DWDM a nižší agregační úrovní tvořenou technologií MPLS. Samotnou agregační vrstvu pak kromě Core routerů vytvoří síť dalších přenosových bodů MPLS, ve kterých budou prováděny sběry příspěvkových signálů z jednotlivých železničních tratí. Tyto přenosy jsou realizovány zejména jako datové s rozhraním Ethernet pomocí Cisco ASR 902 a Cisco ASR 903.

### 3 Související nebo navazujících investiční akce

Stavba navazuje na stavby, které svým charakterem a rozsahem částečně řeší i problematiku této stavby:

- Rekonstrukce a úprava přenosové sítě SŽDC
- Doplnění zařízení a aplikací pro řízení dopravy

**Stavba „*Segmentace provozu v technologické datové síti*“ plně souvisí s výše uvedenými stavbami a realizace této stavby bez výše zmíněných není možná, neboť výše uvedené stavby pro tuto stavbu připravují přenosové prostředí a zařízení dostatečné kapacity při splnění základních požadavků vyplývajících ze zákona č. 181/2014 Sb. - Zákona o kybernetické bezpečnosti ve znění souvisejících předpisů (prováděcí vyhlášky).**

**Pro splnění cílů všech staveb projektant navrhuje realizovat tyto stavby současně s touto stavbou.**

## 4 Základní charakteristika segmentace a jejího užívání

### 4.1 Základní technické řešení

Ve stavbě „Segmentace provozu v technologické datové síti“ bude navržena segmentace provozu v technologické datové síti pomocí VRF/VPN jako základní prostředek pro řízení informačních toků v datové přenosové síti. V rámci segmentace pomocí VRF/VPN bude navržena vzájemná izolace stávajících datových provozů přenosové sítě do samostatných logických celků (VRF/VPN) a to i s výhledem k budoucímu provozu. Dokumentace obsahuje návrh designu a rozdělení provozu (VRF/VPN) podle geografické lokality, funkce nebo typu uživatelů.

Pro zvýšení síťové bezpečnosti na úrovni propojení v rámci jednotlivých Oblastních ředitelství (OŘ) bude navržena ochrana a kontrola přístupu na sdílené SW prostředky v síti Správy železnic, která zvýší kontrolu přístupů a prostupů v rámci správní oblasti (např. OŘ, CDP).

Pro každou správní oblast (OŘ a CDP) budou navrženy dva New Generation Firewally s funkcionalitami AVC (Application Visibility and Control), IDS (Intrusion detection systems), AMP (Advanced Malware Protection). Tyto firewally budou mít za úkol kontrolovat a sledovat provoz jak v rámci oblasti, tak i mezi nimi a provádět řízení politiky v souladu s vnitřními předpisy Správy železnic. Celý soubor firewallů bude řízen a nastavován z dohledového centra.

Cílem stavby je úprava technologické datové sítě ve vztahu k zákonu č. 181/2014 Sb. o kybernetické bezpečnosti a provedení takových úprav, které umožní zajistit vzájemnou izolaci stávajících provozů a případných externích subjektů do samostatné fyzicky nebo logicky oddělené sítě s řízeným prostupem pomocí směrování a TCP/IP komunikačními pravidly.

### 4.2 Rozsah segmentace provozu v TDS

Technické řešení a návrh segmentace provozu v technologické datové síti je rozděleno do níže uvedených PS:

- PS 3-101 OŘ Praha, segmentace provozu
- PS 3-102 OŘ Plzeň, segmentace provozu
- PS 3-103 OŘ Ústí nad Labem, segmentace provozu
- PS 3-104 OŘ Hradec Králové, segmentace provozu
- PS 3-105 OŘ Brno, segmentace provozu
- PS 3-106 OŘ Olomouc, segmentace provozu
- PS 3-107 OŘ Ostrava, segmentace provozu
- PS 3-108 Předimplementační analýza a centrální část

### 4.3 Koncepce technického řešení v navrhované stavbě

Bezpečnost komunikační infrastruktury by se měla v požadavcích na návrh řešení odrážet minimálně v následujících skupinách požadavků:

- Segmentace provozu v technologické datové síti a další architekturní požadavky na síť;
- Zabezpečení přístupu do sítě;
- Podpora subsystémů kybernetické bezpečnosti a potenciál ke splnění aktuálních nebo budoucích legislativních požadavků.

V rámci této stavby bude řešena právě **segmentace provozu v technologické datové síti a podpora subsystémů kybernetické bezpečnosti**. Ostatní kapitoly jsou řešeny souvisejícími investičními akcemi Správy železnic v návaznosti na zákon č. 181/2014 Sb. o kybernetické bezpečnosti.

#### 4.3.1 Segmentace provozu v technologické datové síti

Otevřená a nesegmentovaná technologická datová síť přímo nahrává kybernetickým útokům, které mohou získat snadný přístup k údajům a datům v rámci celé přenosové sítě Správy železnic.

Nesegmentovanou přenosovou síť neohrožují pouze externí hrozby, ale bez oddělení provozu jednotlivých sítí a omezení představují vysoké potenciální riziko i interní hrozby. A není důležité, jestli se jedná o záměrné chování nespokojeného zaměstnance nebo selhání lidského faktoru v podobě nechtěné změny systému.

Z výše popsaných důvodů je velmi důležité provést segmentaci provozu v technologické datové síti.

Pomocí segmentace rozdělíme technologickou datovou síť na několik menších logických celků, kterým je možno přiřadit určitou bezpečnostní úroveň a vytvářet bezpečnostní zóny podle definovaných parametrů. Tím výrazně omezíme bezpečnostní hrozby a zabráníme jejich širšímu dopadu. Segmentací provozu a nastavením příslušných pravidel bude možné zpřístupnit data, činnosti a aplikace, pouze konkrétním subjektům, zaměstnancům atd.

#### 4.3.1.1 Úrovně segmentace

Se segmentací přenosové sítě jsou nejčastěji spojeny virtuální sítě LAN/VLAN. Jedná se o vytvoření zabezpečené virtuální sítě v rámci té existující. Díky VLAN nemusíme přenosovou síť segmentovat fyzicky, ale logicky například podle účelu, organizace či funkce.

Sítě VLAN mohou zařízení a data zabezpečit několika způsoby. Předně můžeme zabránit zařízením v určitých sítích VLAN, aby komunikovala se zařízeními v ostatních sítích VLAN. Dále můžete využít přepínač nebo směrovač s bezpečnostními a filtrovacími funkcemi na úrovni třetí vrstvy a zabezpečit tak komunikaci mezi zařízeními napříč sítěmi VLAN. Přestože jsou sítě VLAN důležitou součástí segmentace, představují pouze jedno řešení. Napříč různými úrovněmi vaší síťové architektury můžete využívat také další metody segmentace. Zjednodušeně lze říct, že VLAN jsou na L2 OSI modelu, které vytvoří základní strukturu a další vrstvy OSI modelu tuto strukturu člení podle potřeby. Napříč různými úrovněmi síťové architektury je možno využívat další metody segmentace.

Jednou z možností je využití demilitarizované zóny (DMZ). Ta vytváří zábranu mezi sítí určenou pro aplikace na úrovni kancelářských činností (např. intranet) a těmi, ve kterých probíhá komunikace nutná pro řízení dopravy (technologická datová síť). Všechny přenosy mezi jednotlivými sítěmi se na této DMZ zastaví, přesto bude možné data dále bezpečně sdílet.

Mezi další využitelné metody segmentace patří tzv. seznam pro řízení přístupu ACL (Access Lists), firewall, virtuální privátní síť (VPN), omezovače pro jednosměrný přenos a systém pro odhalení průniku (IDS).

#### 4.3.1.2 Segmentace infrastruktury

Různorodost požadavků uživatelů aplikací a správců systému i navazujících procesů uživatele vyžaduje výkonné prostředky pro segmentaci sítě jako základní prostředek řízení informačních toků v jejím rámci. V rámci aktuálních trendů zajištění odpovídající segmentace znamená minimálně:

- Použití robustní technologie MPLS (MultiProtocol Label Switching), pro vytváření a provozování bezpečně oddělených a nezávislých VPN pracujících na třetí nebo druhé vrstvě modelu ISO/OSI;
- V případě L3 MPLS VPN dle standardu RFC 2547bis, požadavky na dostatečnou škálovatelnost a flexibilitu i s ohledy na budoucí perspektivy (růst společnosti, organizační změny apod.) – minimální počet zříditelných VPN, možnost definovat VPN sítě se sdílenými datovými zdroji a s konektivitou typu any-to-any nebo hub-and-spoke;
- Možnost vytvářet i L2 MPLS VPN pro transparentní propojení vybraných lokalit, podporu spojnic bod-bod, typů Ethernet, pevná linka apod. s diferencovanými a garantovatelnými QoS;

#### 4.3.2 Podpora subsystémů kybernetické bezpečnosti

Komunikační infrastruktura (KI) musí být maximálně odolná proti bezpečnostním útokům. Z tohoto důvodu musí být nedílnou součástí komunikačních prvků:

- Robustní bezpečnostní mechanismy, které zajistí nejen ochranu přenášených dat, ale rovněž i ochranu samotných komunikačních prvků (firewall systémy atd.);

- Nástroje pro aktivní monitorování datových toků pro účely detekce bezpečnostních incidentů včetně možnosti zasílání monitorovaných dat na centrální systémy, které zajistí kontinuální vyhodnocování bezpečnostních událostí včetně vazby na bezpečnostní systémy;

Uvedené komponenty připravují nově budovanou KI i na požadavky kybernetické ochrany dané nastupující evropskou a současnou národní legislativou, jejíž plná účinnost se očekává během životního cyklu dnes budovaných systémů. Jedná se zejména o Zákon č. 181/2014 Sb., o kybernetické bezpečnosti, který ukládá řadě subjektů, mezi něž se svou důležitostí řadí i drážní prostředí, povinnost zavedení a dodržování bezpečnostních opatření a povinnost hlášení bezpečnostních incidentů. Implementované bezpečnostní prvky proto musí realizovat nebo alespoň musí být rozšiřitelné na plnou podporu požadovaných nástrojů dle ZKB, ke kterým patří:

- fyzická bezpečnost;
- ochrana integrity komunikačních sítí – HW, SW;
- ověřování identity uživatelů včetně přístupu administrátorů;
- řízení přístupových oprávnění včetně přístupu administrátorů;
- ochrana před škodlivým kódem;
- zaznamenávání činnosti kritické informační infrastruktury a významných informačních systémů, jejich uživatelů a správců;
- detekce kybernetických bezpečnostních událostí;
- sběr a vyhodnocení kybernetických bezpečnostních událostí;
- zajištění aplikační bezpečnosti;
- kryptografické prostředky;
- zajišťování úrovně dostupnosti informací;
- bezpečnost průmyslových a řídicích systémů.

Systémy pro administraci by navíc měly obsahovat podporu i pro organizační opatření podle §5 zákona, zejména:

- systém řízení bezpečnosti informací;
- řízení aktiv a rizik;
- bezpečnostní politika;
- organizační bezpečnost;
- stanovení bezpečnostních požadavků na dodavatele;
- řízení provozu a komunikací kritické informační infrastruktury nebo významného informačního systému;
- řízení přístupu osob ke kritické informační infrastruktuře nebo k významnému informačnímu systému;
- zvládání kybernetických bezpečnostních událostí a kybernetických bezpečnostních incidentů;
- řízení kontinuity činností;
- kontrolu a audit kritické informační infrastruktury a významných informačních systémů.

V neposlední řadě by požadavky měly zahrnovat i služby KI pro podporu subsystémů víceúrovňové bezpečnosti a služby KI pro podporu systémů fyzické bezpečnosti.

Komunikační infrastruktura musí umožnit poskytovat síťové služby uvnitř jednotlivých VPN samostatně za individuálních podmínek (přístupové politiky, adresní plány včetně možného překryvu IPv4 adres apod.).



## 5 Návrh technického řešení

Stavba „Segmentace provozu v technologické datové síti“ řeší bezpečné oddělení jednotlivých typů provozu v technologické datové síti do samostatných logických segmentů. Dále řeší zajištění kontrolovaných přístupů mezi jednotlivými logicky izolovanými segmenty. Logická segmentace zachová rovněž možnost připojit a kontrolovat přístupy z fyzicky oddělených segmentů sítě.

Segmentaci bude realizována na různých vrstvách OSI modelu. Na vrstvě L2 prostřednictvím VLAN, na L3 oddělením do samostatných sítí s využitím technologie VRF (Virtual Routing and Forwarding) v MPLS pak označením jednotlivých typů provozu a oddělením do samostatných VPN (Virtual Private Network).

Segmentace je navržena na rozčlenění technologické datové sítě podle druhu přenášeného provozu, případně je určena technologií nebo typem zařízení pro kterou je daný segment vyhrazen. Tyto logické segmenty určené typem přenášených dat jsou následně segmentovány geograficky podle příslušnosti k OŘ. Další úrovní je hierarchická segmentace, kdy provoz z jednotlivých OŘ přechází do příslušného segmentu páteřní (globální) sítě. Tento princip tak umožňuje minimalizaci L2 segmentů, optimalizaci L3 segmentů a zajišťuje možnost kontroly a řízení provozu mezi jednotlivými segmenty. Z hlediska správy dovolí segmentace při vhodné implementaci řídit provoz v síti na základě relativně malých segmentů, které tak v případě bezpečnostního nebo provozního incidentu nebudou nevhodně ovlivňovat provoz v ostatních segmentech.

S ohledem na předpokládaný rozsah segmentace je nutné, aby byly náležitě dimenzovány síťové prvky přenosové sítě, zejména s ohledem na podporu dostatečného množství VRF, lze očekávat požadavky až v desítkách VRF.

Detaily návrhu a popis technického řešení jsou uvedeny dále.

### 5.1 Segmenty

Segmenty budou tvořeny logicky na základě typu provozu, resp. technologického určení (např. hlas, video atp.) a zároveň geograficky podle umístění připojovaného zařízení nebo uživatele v síti.

Členění řešeno následovně:

| Technologie  | Virtuální síť<br>IP/MPLS |
|--|--------------------------|
| Kontrolně-analytické centrum řízení provozu/Jednotné záznamové prostředí   | VOICE                    |
| Hlasové servery, MRTS a dispečerské terminály, gateway (do GSM-R nebo ŽSTS), CCM a srst routery, MB/IP převodníky atd. | VOICE                    |
| ZPDP, PZTS   | DIAG                     |
| Dohled základnových radiostanic  | DIAG                     |
| Kamery pro řízení provozu (liniové)  | CCTV                     |
| Kamery pro správu elektrotechniky a energetiky   | CCTV                     |
| Kamery pro řízení provozu (velké žst.), Elektronické zobrazovací panely  | CCTV                     |
| Kamery pro řízení provozu (velké žst.)   | CCTV                     |
| IS pro cestující   | VOICE                    |
| EOV diagnostika  | DIAG                     |
| EOV parametrizace  | DIAG                     |
| ZPDP, PZTS parametrizace<br>ZPDP, PZTS parametrizace pro SEE   | DIAG                     |
| IP telefony a PBX služební telefonní síť   | ZSTS                     |
| DŘT  | DRT                      |



|   |         |
|---|---------|
| DŘT záložní přenosy pro trakční napájecí stanice                      | DRT     |
| DŘT, Elektroměry Odboru energetiky a služeb OŘ                        | MARSEE  |
| Kotelny, vzduchotechnika  | DIAG    |
| Kolejové váhy   | DIAG    |
| InK, InS, klienti   | DIAG    |
| Lokální síť pro přenosy GSM-R v rámci DDTS                            | DIAG    |
| Diagnostika jedoucích železničních vozidel, kontrola sběračů          | DIAG    |
| Provozní aplikace pro vedení dopravní dokumentace                     | DOPR    |
| Kamery v budovách (mimo technologické prostory), Kamery na přejezdech | VSS     |
| ETCS  | ETCS    |
| Diagnostika TLS – LTDS  | DIAG    |
| Diagnostika zabezpečovacího zařízení v TDS                            | DIAG    |
| Switche kamerových systémů  | DIAG    |
| Switche, routery, modemy  | DOHLED  |
| zdroje, UPS   | DOHLED  |
| ONS   | DOHLED  |
| RAD Megaplex  | DOHLED  |
| Správa hlasových serverů  | ILOSERV |
| IP ústředny, správa zapojovačů  | ILOSERV |
| Zdroje, UPS   | DIAG    |
| Správa virtualizačních serverů  | ILOSERV |
| Správa serverů diagnostiky zabezpečovacího zařízení                   | ILOSERV |
| Správa serverů provozních aplikací pro vedení dopravní dokumentace    | ILOSERV |

Tab. 1 – Členění segmentů podle technologie

Segmenty podle geografického umístění:

- Podle OŘ
  - OŘ Praha
  - OŘ Plzeň
  - OŘ Ústí nad Labem
  - OŘ Hradec Králové
  - OŘ Brno
  - OŘ Olomouc
  - OŘ Ostrava
- Specifické segmenty dle potřeby, např.
  - CDP Praha
  - CDP Přerov
  - Datová Centra
  - Georedundance
  - atd.
- Globální (páteří síť) propojující OŘ

Díky výše uvedenému členění je možné oddělit a řídit datový provoz jak podle druhu přenášeného provozu, tak i podle příslušnosti k určitému OŘ. Kontrola provozu bude prováděna vždy na hranicích mezi jednotlivými segmenty viz dále.

Pravidla pro definování segmentů dle typu provozu:

- 1) Segment je určen typem provozu, resp. technologií která se má v daném segmentu VPN/VRF oddělit.
- 2) Číslo, resp. název segmentu je stejný pro globální i OŘ část sítě. V názvu se pouze vhodně odliší příslušnost k OŘ nebo do globální sítě. V následující tabulce jsou uvedena pravidla pro přechod provozu mezi jednotlivými segmenty.
- 3) Určení v bodě výše je aplikováno stejně v sítích OŘ i v globální části sítě.

Pravidla pro definování segmentů dle geografického umístění:

- 1) Příslušnost k OŘ je dána geografickým umístěním zařízení, portu nebo dedikovaním zařízení pro dané OŘ např. při umístění v zařízení v lokalitách mimo OŘ např. v centrálních datových centrech z důvodu redundance.
- 2) VRF jsou definovány pro jednotlivá OŘ, případně další lokality např. CDP, DC atp. dle současných, resp. budoucích požadavků.
- 3) Při přechodu datového spoje mezi různými OŘ je třeba dodržovat příslušnost k danému OŘ. Na hranicích je třeba umísťovat vhodné prvky (PE) routery.

Pravidla pro přechod mezi segmenty:

| Segment             | VRF v OŘ  | VRF globální   |
|---------------------|---|--|
| <b>VRF v OŘ</b>     | Přechod mezi různými VRF v daném OŘ je povolen pouze přes prostup kontrolovaný firewallem určeným pro dané OŘ.  | Prostup z určitého VRF v OŘ je umožněn pouze do stejného typu globální VRF (tzn. např. z hlas v OŘ do hlas v globální síti). Přechod do globálního VRF určeného pro jiný typ provozu není povolen! |
| <b>VRF globální</b> | Prostup z určitého VRF v globální síti do VRF v OŘ je umožněn pouze do stejného typu VRF v OŘ (tzn. např. z hlas v OŘ do hlas v globální síti). Přechod do VRF v OŘ určeného pro jiný typ provozu není povolen! | Přechod provozu mezi různými globálními VRF je povolen pouze přes prostup kontrolovaný globálním firewallem.   |

Tab. 2 – Pravidla pro přechod mezi segmenty

## 5.2 Škálovatelnost segmentace

S ohledem na rozvoj sítě a nároků na bezpečnost je třeba zajistit, aby byla zajištěna možnost sítí segmentovat i s ohledem na budoucí rozvoj. Z tohoto důvodu je třeba instalovat taková zařízení, aby byla po dobu své životnosti schopna zajistit segmentaci minimálně v následujícím rozsahu:

- Počet VRF v jednom OŘ minimálně 50
- Počet VPN VRF v globální části sítě minimálně 50
- Počet prefixů (adresních rozsahů) minimálně 10 000 v každém globální VRF
- Kompatibilita se stávajícím zařízeními v síti SŽ, tj. zejména s routery Cisco ASR 9xx, Cisco FP21xx a FP41xx, atd.
- Možnost variabilního umístění firewallů s ohledem na topologii přenosové sítě.

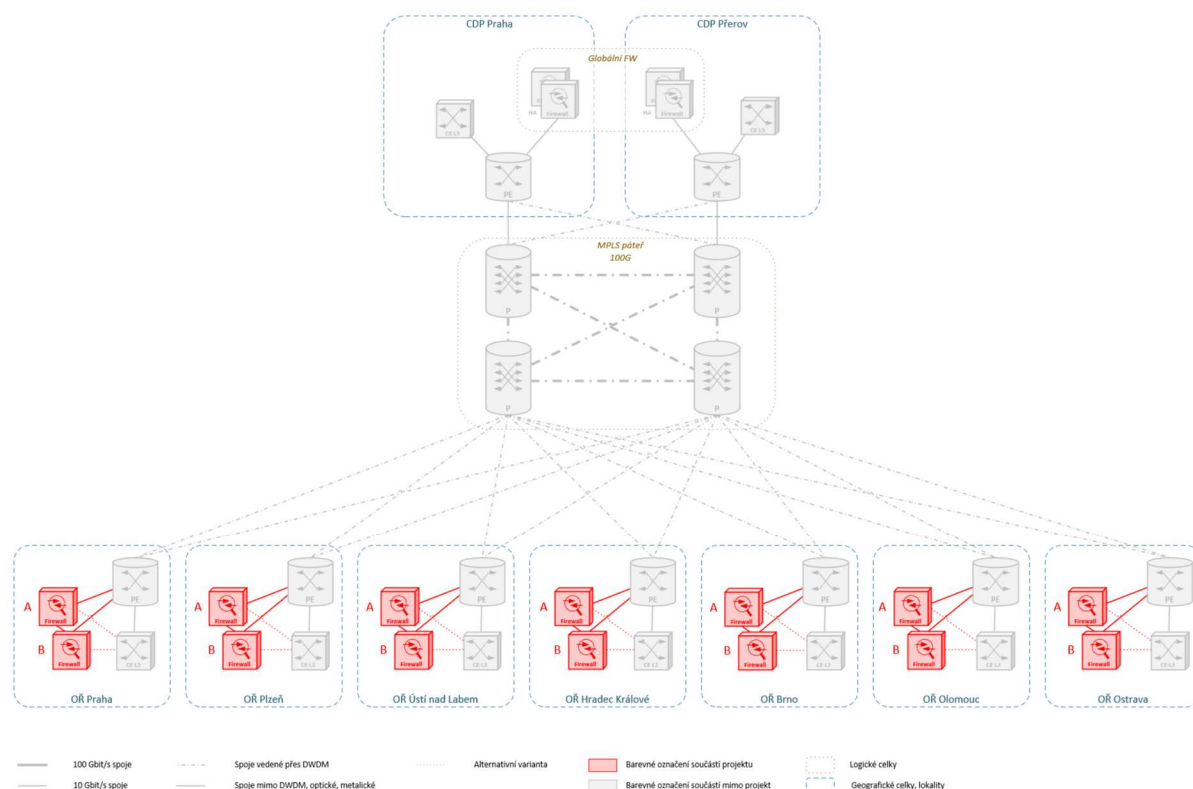
V rámci této stavby budou v každém OŘ umístěny redundantní bezpečnostní prvky provozované v režimu vysoké dostupnosti.

### 5.3 Architektura segmentace

Pro umožnění segmentace je potřeba mít k dispozici dostatečně dimenzovanou přenosovou síť jak z hlediska propustnosti, tak i topologického pokrytí území a dostatečné výkonosti prvků. Tato funkcionality bude řešena v rámci souběžné stavby „*Rekonstrukce a úprava přenosové sítě SŽDC*“.

Stavba „*Segmentace provozu v technologické datové síti*“ využívá stávající infrastrukturu a řeší úpravu konfigurací s ohledem na změny adresování a změny v topologii stávajících segmentů, např. rozdělování sítě na menší L2 segmenty a zajištění jejich směrování.

Fyzicky bude segmentace realizována na redundantních bezpečnostních prvcích umístěných v daném OŘ a provozovaných v režimu vysoké dostupnosti. Bezpečnostní prvky musí umožňovat práci v L3 režimu.



Obr. 1 – Architektura segmentace provozu

Firewally v OŘ budou připojeny ke stávajícím PE routerům řady Cisco ASR, případně nově budovaným v rámci projektu „*Rekonstrukce a úprava přenosové sítě SŽDC*“. Variantně musí být možné připojení bezpečnostních prvků místo do PE do CE routerů. Připojení FW bude realizováno 10G spoji. Propojení bude realizováno prostřednictvím optických SFP modulů.

### 5.4 Řízení prostupů na FW

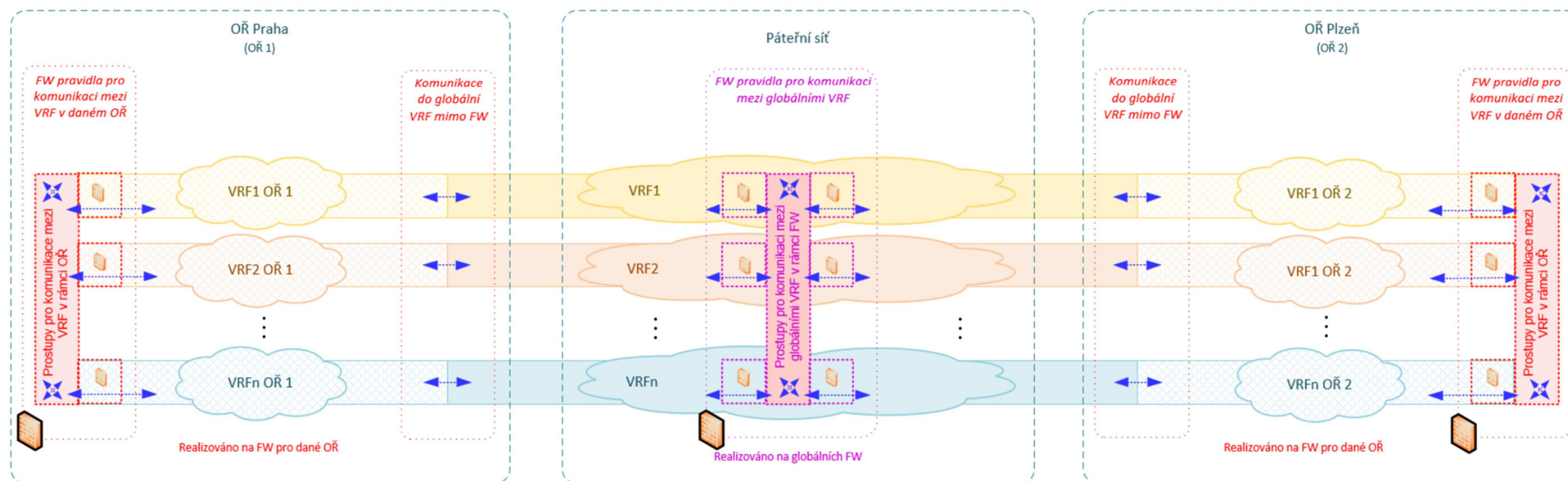
Logické schéma a komunikační matice viz níže znázorňuje princip segmentace a vysvětluje význam jednotlivých firewallů a rovněž znázorňuje druhy komunikace, které je možno na FW povolovat a které jsou zakázány.

Bezpečnostní prvky (firewally) v OŘ kontrolují komunikaci mezi různými VRF v daném OŘ. Komunikace mezi VRF stejného určení v OŘ a globální síti je povolena a není kontrolována FW v OŘ. Komunikace mezi VRF různého určení v OŘ a v globální síti není povolena.

Globální firewall kontroluje komunikaci mezi globálními VRF, tj. pokud je třeba povolit provoz mezi VRF různého určení v globální části sítě. Prostup mezi globálním VRF nesmí být umožněn nikde jinde než na globálních firewallech.

## Logické schéma komunikace

Princip oddělení a zabezpečení komunikace v rámci OŘ a mezi OŘ a páteřní (globální) sítí



### Seznam OŘ

- 1: OŘ Praha
- 2: OŘ Plzeň
- 3: OŘ Ústí nad Labem
- 4: OŘ Hradec Králové
- 5: OŘ Brno
- 6: OŘ Olomouc
- 7: OŘ Ostrava

### Seznam VRF (globální a OŘ)

- VRF1 (CCTV)
- VRF2 (DIAG)
- VRF3 (DOHLED)
- VRF4 (DOPR)
- VRF5 (DRT)
- VRF6 (ETCS)
- VRF7 (ILOSERV)
- VRF8 (MARSEE)
- VRF9 (VOICE)
- VRF10 (VSS)
- VRF11 (ZSTS)

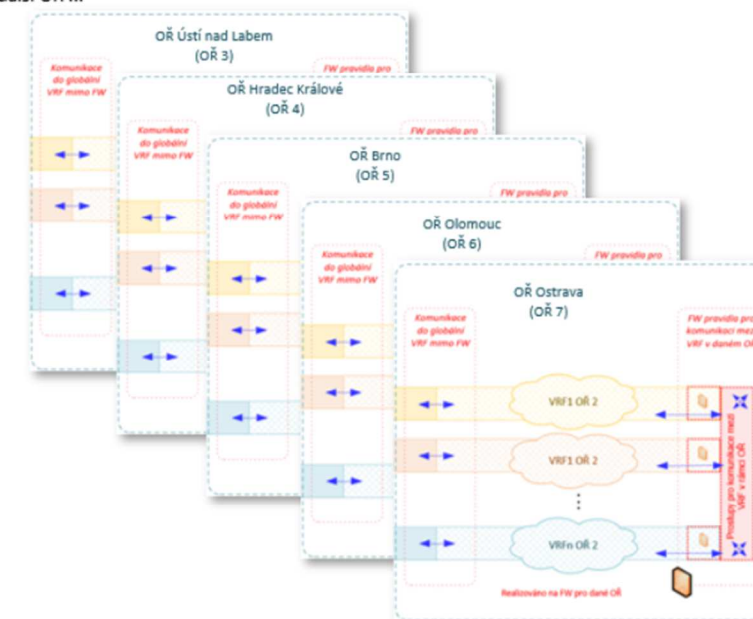
### Segmentace sítě:

- VPN v rámci páteřní sítě (VRF globální)
- VPN v rámci OŘ (VRF OŘ)

### Segmentace (určení) firewallů:

- globální FW, určené pro kontrolu komunikace mezi globálními VPN (VRF)
- FW v OŘ určené pro kontrolu komunikace mezi VRF v rámci OŘ

Obdobně pro další OŘ ...



- Logické celky
- Geografické celky, lokality

- VRF1 VRF (VPN) v rámci OŘ VRF(x) OŘ (y), x je číslo VRF, y je číslo OŘ
- VRF1 VRF (VPN) v rámci páteřní (globální) sítě VRF(x), x je číslo VRF

- Aplikování pravidel na FW OŘ pro přístup mezi různými VRF v rámci OŘ
- Aplikování pravidel na globálním FW pro přístup mezi různými globálními VRF v páteřní síti



## 5.5 Komunikační pravidla, matice

Možné varianty komunikace jsou zahrnuté v následující matici.

### Komunikační pravidla, komunikační matice

Princip kontroly komunikace mezi VRF v oblasti kontrolované FW v OŘ a VRF v páteřní (globální) síti

Výřez matice pro komunikaci mezi VRF

| Komunikační matice |                 | Komunikace – strana A |             |               |             |            |             |                |               |              |             |               |              | Komunikace – strana B    |              |                |              |             |              |                 |                |               |             |               |              |
|--------------------|-----------------|-----------------------|-------------|---------------|-------------|------------|-------------|----------------|---------------|--------------|-------------|---------------|--------------|--------------------------|--------------|----------------|--------------|-------------|--------------|-----------------|----------------|---------------|-------------|---------------|--------------|
| VRF                | VRF             | FW pro OŘ Praha       |             |               |             |            |             |                |               |              |             |               |              | FW pro OŘ Ústí nad Labem |              |                |              |             |              |                 |                |               |             |               |              |
|                    |                 | VRF1 (CCTV)           | VRF2 (DIAG) | VRF3 (DOHLED) | VRF4 (DOPR) | VRF5 (DRT) | VRF6 (ETCS) | VRF7 (ILOSERV) | VRF8 (MARSEE) | VRF9 (VOICE) | VRF10 (VSS) | VRF11 (ZSTIS) | VRF12 (CCTV) | VRF13 (CCTV)             | VRF14 (DIAG) | VRF15 (DOHLED) | VRF16 (DOPR) | VRF17 (DRT) | VRF18 (ETCS) | VRF19 (ILOSERV) | VRF20 (MARSEE) | VRF21 (VOICE) | VRF22 (VSS) | VRF23 (ZSTIS) | VRF24 (CCTV) |
| VRF1 (CCTV)        | VRF1 (CCTV)     | X                     |             |               |             |            |             |                |               |              |             |               |              | X                        |              |                |              |             |              |                 |                |               |             |               |              |
| VRF2 (DIAG)        | VRF2 (DIAG)     | X                     | X           |               |             |            |             |                |               |              |             |               |              | X                        | X            |                |              |             |              |                 |                |               |             |               |              |
| VRF3 (DOHLED)      | VRF3 (DOHLED)   | X                     | X           | X             |             |            |             |                |               |              |             |               |              | X                        | X            | X              |              |             |              |                 |                |               |             |               |              |
| VRF4 (DOPR)        | VRF4 (DOPR)     | X                     | X           | X             | X           |            |             |                |               |              |             |               |              | X                        | X            | X              | X            |             |              |                 |                |               |             |               |              |
| VRF5 (DRT)         | VRF5 (DRT)      | X                     | X           | X             | X           | X          |             |                |               |              |             |               |              | X                        | X            | X              | X            | X           |              |                 |                |               |             |               |              |
| VRF6 (ETCS)        | VRF6 (ETCS)     | X                     | X           | X             | X           | X          | X           |                |               |              |             |               |              | X                        | X            | X              | X            | X           | X            |                 |                |               |             |               |              |
| VRF7 (ILOSERV)     | VRF7 (ILOSERV)  | X                     | X           | X             | X           | X          | X           | X              |               |              |             |               |              | X                        | X            | X              | X            | X           | X            | X               |                |               |             |               |              |
| VRF8 (MARSEE)      | VRF8 (MARSEE)   | X                     | X           | X             | X           | X          | X           | X              | X             |              |             |               |              | X                        | X            | X              | X            | X           | X            | X               | X              |               |             |               |              |
| VRF9 (VOICE)       | VRF9 (VOICE)    | X                     | X           | X             | X           | X          | X           | X              | X             | X            |             |               |              | X                        | X            | X              | X            | X           | X            | X               | X              | X             |             |               |              |
| VRF10 (VSS)        | VRF10 (VSS)     | X                     | X           | X             | X           | X          | X           | X              | X             | X            | X           |               |              | X                        | X            | X              | X            | X           | X            | X               | X              | X             | X           |               |              |
| VRF11 (ZSTIS)      | VRF11 (ZSTIS)   | X                     | X           | X             | X           | X          | X           | X              | X             | X            | X           | X             |              | X                        | X            | X              | X            | X           | X            | X               | X              | X             | X           | X             |              |
| VRF12 (CCTV)       | VRF12 (CCTV)    | X                     | X           | X             | X           | X          | X           | X              | X             | X            | X           | X             | X            | X                        | X            | X              | X            | X           | X            | X               | X              | X             | X           | X             | X            |
| VRF13 (CCTV)       | VRF13 (CCTV)    | X                     | X           | X             | X           | X          | X           | X              | X             | X            | X           | X             | X            | X                        | X            | X              | X            | X           | X            | X               | X              | X             | X           | X             | X            |
| VRF14 (DIAG)       | VRF14 (DIAG)    | X                     | X           | X             | X           | X          | X           | X              | X             | X            | X           | X             | X            | X                        | X            | X              | X            | X           | X            | X               | X              | X             | X           | X             | X            |
| VRF15 (DOHLED)     | VRF15 (DOHLED)  | X                     | X           | X             | X           | X          | X           | X              | X             | X            | X           | X             | X            | X                        | X            | X              | X            | X           | X            | X               | X              | X             | X           | X             | X            |
| VRF16 (DOPR)       | VRF16 (DOPR)    | X                     | X           | X             | X           | X          | X           | X              | X             | X            | X           | X             | X            | X                        | X            | X              | X            | X           | X            | X               | X              | X             | X           | X             | X            |
| VRF17 (DRT)        | VRF17 (DRT)     | X                     | X           | X             | X           | X          | X           | X              | X             | X            | X           | X             | X            | X                        | X            | X              | X            | X           | X            | X               | X              | X             | X           | X             | X            |
| VRF18 (ETCS)       | VRF18 (ETCS)    | X                     | X           | X             | X           | X          | X           | X              | X             | X            | X           | X             | X            | X                        | X            | X              | X            | X           | X            | X               | X              | X             | X           | X             | X            |
| VRF19 (ILOSERV)    | VRF19 (ILOSERV) | X                     | X           | X             | X           | X          | X           | X              | X             | X            | X           | X             | X            | X                        | X            | X              | X            | X           | X            | X               | X              | X             | X           | X             | X            |
| VRF20 (MARSEE)     | VRF20 (MARSEE)  | X                     | X           | X             | X           | X          | X           | X              | X             | X            | X           | X             | X            | X                        | X            | X              | X            | X           | X            | X               | X              | X             | X           | X             | X            |
| VRF21 (VOICE)      | VRF21 (VOICE)   | X                     | X           | X             | X           | X          | X           | X              | X             | X            | X           | X             | X            | X                        | X            | X              | X            | X           | X            | X               | X              | X             | X           | X             | X            |
| VRF22 (VSS)        | VRF22 (VSS)     | X                     | X           | X             | X           | X          | X           | X              | X             | X            | X           | X             | X            | X                        | X            | X              | X            | X           | X            | X               | X              | X             | X           | X             | X            |
| VRF23 (ZSTIS)      | VRF23 (ZSTIS)   | X                     | X           | X             | X           | X          | X           | X              | X             | X            | X           | X             | X            | X                        | X            | X              | X            | X           | X            | X               | X              | X             | X           | X             | X            |
| VRF24 (CCTV)       | VRF24 (CCTV)    | X                     | X           | X             | X           | X          | X           | X              | X             | X            | X           | X             | X            | X                        | X            | X              | X            | X           | X            | X               | X              | X             | X           | X             | X            |
| VRF25 (DIAG)       | VRF25 (DIAG)    | X                     | X           | X             | X           | X          | X           | X              | X             | X            | X           | X             | X            | X                        | X            | X              | X            | X           | X            | X               | X              | X             | X           | X             | X            |
| VRF26 (DOHLED)     | VRF26 (DOHLED)  | X                     | X           | X             | X           | X          | X           | X              | X             | X            | X           | X             | X            | X                        | X            | X              | X            | X           | X            | X               | X              | X             | X           | X             | X            |
| VRF27 (DOPR)       | VRF27 (DOPR)    | X                     | X           | X             | X           | X          | X           | X              | X             | X            | X           | X             | X            | X                        | X            | X              | X            | X           | X            | X               | X              | X             | X           | X             | X            |
| VRF28 (DRT)        | VRF28 (DRT)     | X                     | X           | X             | X           | X          | X           | X              | X             | X            | X           | X             | X            | X                        | X            | X              | X            | X           | X            | X               | X              | X             | X           | X             | X            |
| VRF29 (ETCS)       | VRF29 (ETCS)    | X                     | X           | X             | X           | X          | X           | X              | X             | X            | X           | X             | X            | X                        | X            | X              | X            | X           | X            | X               | X              | X             | X           | X             | X            |
| VRF30 (ILOSERV)    | VRF30 (ILOSERV) | X                     | X           | X             | X           | X          | X           | X              | X             | X            | X           | X             | X            | X                        | X            | X              | X            | X           | X            | X               | X              | X             | X           | X             | X            |
| VRF31 (MARSEE)     | VRF31 (MARSEE)  | X                     | X           | X             | X           | X          | X           | X              | X             | X            | X           | X             | X            | X                        | X            | X              | X            | X           | X            | X               | X              | X             | X           | X             | X            |
| VRF32 (VOICE)      | VRF32 (VOICE)   | X                     | X           | X             | X           | X          | X           | X              | X             | X            | X           | X             | X            | X                        | X            | X              | X            | X           | X            | X               | X              | X             | X           | X             | X            |
| VRF33 (VSS)        | VRF33 (VSS)     | X                     | X           | X             | X           | X          | X           | X              | X             | X            | X           | X             | X            | X                        | X            | X              | X            | X           | X            | X               | X              | X             | X           | X             | X            |
| VRF34 (ZSTIS)      | VRF34 (ZSTIS)   | X                     | X           | X             | X           | X          | X           | X              | X             | X            | X           | X             | X            | X                        | X            | X              | X            | X           | X            | X               | X              | X             | X           | X             | X            |
| VRF35 (CCTV)       | VRF35 (CCTV)    | X                     | X           | X             | X           | X          | X           | X              | X             | X            | X           | X             | X            | X                        | X            | X              | X            | X           | X            | X               | X              | X             | X           | X             | X            |
| VRF36 (DIAG)       | VRF36 (DIAG)    | X                     | X           | X             | X           | X          | X           | X              | X             | X            | X           | X             | X            | X                        | X            | X              | X            | X           | X            | X               | X              | X             | X           | X             | X            |
| VRF37 (DOHLED)     | VRF37 (DOHLED)  | X                     | X           | X             | X           | X          | X           | X              | X             | X            | X           | X             | X            | X                        | X            | X              | X            | X           | X            | X               | X              | X             | X           | X             | X            |
| VRF38 (DOPR)       | VRF38 (DOPR)    | X                     | X           | X             | X           | X          | X           | X              | X             | X            | X           | X             | X            | X                        | X            | X              | X            | X           | X            | X               | X              | X             | X           | X             | X            |
| VRF39 (DRT)        | VRF39 (DRT)     | X                     | X           | X             | X           | X          | X           | X              | X             | X            | X           | X             | X            | X                        | X            | X              | X            | X           | X            | X               | X              | X             | X           | X             | X            |
| VRF40 (ETCS)       | VRF40 (ETCS)    | X                     | X           | X             | X           | X          | X           | X              | X             | X            | X           | X             | X            | X                        | X            | X              | X            | X           | X            | X               | X              | X             | X           | X             | X            |

#### Globální firewall:

- povoluje pouze protupy mezi různými typy globálních VRF v páteřní síti!

#### Firewally v OŘ:

- povolují protupy mezi různými typy VRF v rámci OŘ
- Komunikace do stejného VRF v globální síti není FW kontrolována. Prostup do jiného globálního VRF není povolen. Protupy mezi různými typy globálních VRF jsou povoleny pouze na globálních firewalllech.

Komunikace je řízena pravidly na globálním firewallu

Komunikace mimo kontrolu FW v globální síti

Komunikace je řízena pravidly na firewallu v OŘ

Komunikace mimo kontrolu FW v OŘ

Komunikace není povolena!

Obr. 2 – Příklad komunikační matice, komunikační pravidla

## 5.6 Dimenzování firewallů

Navržené firewally musí být dimenzovány pro propustnost 10Gbit (přesná specifikace je níže) s 10GE SFP+ rozhraními. FW musí podporovat provoz v HA v režimu active/active i active/passive a musí být dodány se všemi nezbytnými licencemi pro provozování. Z hlediska záruky a podpory výrobce je požadováno:

- Záruka na HW na 60 měsíců
- Podpora výrobce (SmartNet nebo obdobné) na 24 měsíců
- Subskripce pro všechny SW licence na dobu minimálně 36 měsíců

Použité bezpečnostní prvky (firewally) musí splňovat minimálně následující technické parametry:

- Výška 1U
- Redundantní napájení ve variantách s 2x 230V AC nebo 2x 48V DC napájecími zdroji
- Minimální počet 4x 10GE SFP+ a 12x GE portů jako součást šasi (možnost rozšíření až na celkový počet 12x 10GE SFP+)
- Slot pro přídatný (rozšiřující) modul síťových rozhraní (až do souhrnného počtu 24 portů)
- Minimální propustnost stavového firewallu 10 Gbit/s
- Minimální propustnost firewallu 5 Gbit/s
- Minimální počet současných spojení 1 900 000
- Rychlost sestavení nových spojení minimálně 38 000
- Požadovaný počet bezpečnostních kontextů 2
- Možnost rozšíření počtu bezpečnostních kontextů až na 27
- Pokročilé funkce ochrany proti malware, detekce průniku do sítě a application visibility
- Firewally musí umožňovat funkci HA včetně geografické redundance a podporovat režim active/active tak i active/passive.
- Správa přes centrální management

## 5.7 PS 3-101 OŘ Praha, segmentace provozu

## 5.8 PS 3-102 OŘ Plzeň, segmentace provozu

## 5.9 PS 3-103 OŘ Ústí nad Labem, segmentace provozu

## 5.10 PS 3-104 OŘ Hradec Králové, segmentace provozu

## 5.11 PS 3-105 OŘ Brno, segmentace provozu

## 5.12 PS 3-106 OŘ Olomouc, segmentace provozu

## 5.13 PS 3-107 OŘ Ostrava, segmentace provozu

V rámci těchto PS se navrhuje ochrana a kontrola přístupu na sdílené prostředky v síti Správy železnic v rámci jednotlivých oblastních ředitelství (OŘ). Ochrana a kontrola bude spočívat ve výstavbě nových FireWallů (FW) s potřebnými funkcionalitami pro kontrolu sledování provozu, a to jak v příslušném OŘ, tak i mezi nimi. Realizaci těchto FW bude zajištěna možnost provádět řízení politiky sítě.

Do vybraných lokalit v rámci OŘ budou navrženy dva New Generation FW s funkcionalitami AVC, IDS, AMP v redundantním řešení a dle provozu v příslušném OŘ bude nastavena politika řízení. Tyto FW budou mít za úkol kontrolovat a sledovat provoz v rámci oblasti OŘ a provádět řízení politiky v souladu s vnitřními předpisy Správy železnic.

Celý soubor firewallů bude řízen a nastavován z dohledového centra. Přístupové CE L3 switch se předpokládá dodat související stavbou „*Rekonstrukce a úprava přenosové sítě SŽDC*“.



| OŘ                | ŽST/Lokalita              | Objekt                         |
|-------------------|---------------------------|--------------------------------|
| OŘ Praha          | Balabenka                 | CDP Praha                      |
| OŘ Plzeň          | ŽST Plzeň hl. n.          | Ústřední stavědlo triangl      |
| OŘ Ústí nad Labem | ŽST Ústí n. Labem – sever | Ústřední stavědlo              |
| OŘ Hradec Králové | ŽST Pardubice hl. n.      | Provozní objekt pražské zhlaví |
| OŘ Brno           | Brno – Maloměřice         | Provozní objekt                |
| OŘ Olomouc        | ŽST Přerov                | CDP Přerov                     |
| OŘ Ostrava        | ŽST Ostrava-Svinov        | Výpravní budova                |

Obr. 3 – Seznam lokalit

Dodávkou těchto New Generation Firewallu bude zajištěno zvýšení síťové bezpečnosti na úrovni propojení v rámci jednotlivých OŘ bude navržena ochrana a kontrola přístupu na sdílené SW prostředky v síti Správy železnic, která zvýší kontrolu přístupů a prostupů v rámci správní oblasti.

### 5.13.1 Umístění zařízení

#### 5.13.1.1 OŘ Praha – oblast Balabenka, CDP Praha

V oblasti OŘ Praha bude dvojice FW v HA provedení instalována ve sdělovací místnosti (2.11) v objektu CDP Praha. Zařízení budou instalována do stávajícího 19" racku umístěného ve 1.stojanové řadě s označením 01-06. V 19" racku je umístěn stávající PE router ASR 903 a zařízení DWDM.

Napájení bude řešeno ze stávajícího napájecího zdroje Benning, který je umístěn ve sdělovací místnosti. V 19" skříní 01-06 je osazen stávající zásuvkový, distribuční a jističový panel 48V DC, který bude doplněn pro potřeby napájení dvou FW (jističe).

#### 5.13.1.2 OŘ Plzeň – ŽST Plzeň hl. n., Ústřední stavědlo triangl

V oblasti OŘ Plzeň bude dvojice FW v HA provedení instalována ve sdělovací místnosti (1.11) v ústředním stavědle triangl v ŽST Plzeň hl. nádraží. Zařízení budou instalována do stávajícího 19" racku umístěného ve 1.stojanové řadě s označením 01-06. V 19" racku je umístěn stávající PE router ASR 903 (který bude v rámci stavby „Rekonstrukce a úprava přenosové sítě SŽDC“) a zařízení DWDM.

Napájení bude řešeno ze stávajícího napájecího zdroje Benning, který je umístěn ve sdělovací místnosti. V rámci návazné stavby výše uvedené modernizace bude zdroj doplněn jedním modulem 48VDC/3kW a vyměněna stávající akubaterie. V 19" skříní 01-06 je osazen stávající distribuční a jističový panel 48V DC dvousektorový, který bude doplněn pro potřeby napájení dvou FW čtyřmi jističi (vždy dva jednom sektoru) o jistícím proudu 10A/1 DC.

#### 5.13.1.3 OŘ Ústí nad Labem – ŽST Ústí nad Labem-sever, Ústřední stavědlo

V oblasti OŘ Ústí nad Labem bude dvojice FW v HA provedení instalována ve sdělovací místnosti v objektu ústředního stavědla v ŽST Ústí nad Labem – obvod sever ve 2.NP. Zařízení budou instalována do stávajícího 19" racku umístěného ve 2.stojanové řadě s označením R02/04. V 19" racku je umístěn stávající PE router ASR 903 a zařízení DWDM.

Napájení bude řešeno ze stávajícího napájecího zdroje Benning, který je umístěn ve sdělovací místnosti. V 19" skříní 02-04 je osazen stávající distribuční a jističový panel 48V DC, který bude doplněn pro potřeby napájení dvou FW čtyřmi jističi (vždy dva jednom sektoru) o jistícím proudu 10A/1 DC. Úprava napájecího zdroje bude řešena v související stavbě „Rekonstrukce a úprava přenosové sítě SŽDC“.

#### 5.13.1.4 OŘ Hradec Králové – ŽST Pardubice hl. n., Provozní budova

Dvojice FW v HA provedení s potřebnými funkcionalitami bude v OŘ Hradec Králové umístěna v ŽST Pardubice hl. n. v novém provozním objektu na pražském zhlaví ve sdělovací místnosti (1.12). Tento provozní objekt bude realizován stavbu „Modernizace železničního uzlu Pardubice“. FW budou umístěny do 19“ rackové skříně 01-02, které budou dodány v rámci související stavby uzlu Pardubice včetně napájecích zdrojů. Do rozjišťovacího panelu 48VDC budou umístěny 4 jističe 10A/1 DC do dvou sektorů napájení.

#### 5.13.1.5 OŘ Brno – Brno Maloměřice, Provozní objekt

Umístění zařízení v OŘ Brno bude ve stávajícím objektu ATÚ Brno Maloměřice v telekomunikační místnosti. Dvojice FW v HA provedení bude dodána do stávajícího 19“ racku s označením 02\_03, ve kterém je umístěn PE router ASR 903.

Napájení bude řešeno ze stávajícího napájecího zdroje Benning, který je umístěn ve vedlejší řadě. V 19“ skříně 03\_04 je osazen stávající distribuční a jističový panel 48V DC, který bude doplněn pro potřeby napájení dvou FW (jističe).

#### 5.13.1.6 OŘ Olomouc – ŽST Přerov, CDP Přerov

V oblasti OŘ Olomouc bude dvojice FW v HA provedení instalována ve sdělovací místnosti č. 2.17 v objektu CDP Přerov. Zařízení budou instalována do stávajícího 19“ racku umístěného ve 4.stojanové řadě s označením D4. V 19“ racku je umístěn stávající PE router ASR 903 a zařízení DWDM.

Napájení bude řešeno ze stávajícího napájecího zdroje Benning, který je umístěn ve 2.stojanové řadě. V 19“ skříně D4 je osazen stávající distribuční a jističový panel 48V DC, který bude doplněn pro potřeby napájení dvou FW (jističe). Pro napájení FW budou doplněny jističe a zásuvkový panel.

#### 5.13.1.7 OŘ Ostrava – ATÚ Ostrava Svinov

V oblasti OŘ Ostrava bude dvojice FW v HA provedení instalována v ŽST Ostrava-Svinov ve výpravní budově v telekomunikační místnosti č.127. Zařízení budou instalována do stávajícího 19“ racku umístěného ve 1.stojanové řadě s označením 01\_03. V 19“ racku je umístěn stávající PE router ASR 903 a zařízení DWDM.

Napájení bude řešeno ze stávajícího napájecího zdroje Benning, který je umístěn v telekomunikační místnosti. V 19“ skříně 01\_03 je osazen stávající distribuční a jističový panel 48V DC, který bude doplněn pro potřeby napájení dvou FW (jističe).

### 5.14 PS 3-108 Předimplementační analýza a centrální části

Segmentace provozu v technologické datové síti bude řešena, jak bylo již výše uvedeno pomocí VRF/VPN. V rámci tohoto PS bude provedena konfigurace, parametrizace a samotná vzájemná izolace stávajících datových provozů v TDS na samostatné logické celky (VRF/VPN) i s výhledem k budoucímu provozu v TDS.

V rámci tohoto PS bude provedena:

- Analýza provozu v technologické datové síti (definice provozů, ...)
- Stanovení segmentů, komunikace a pravidla segmentace
- Postupné provádění technologické a topologické segmentace

Bude provedena technologická a topologická segmentace prezentována v kapitolách výše. Po provedení segmentace provozu v TDS se očekává v rámci přenosové sítě Správy železnic minimalizace L2 segmentů (tzn. omezení broadcast domén a L2 segmenty mít v co nejmenším rozsahu a k přenosu využívat primárně L3), větší bezpečnost, kontrola provozu, omezení šíření chyb, minimalizace broadcast domén a zvýšení robustnosti bezpečnosti v rámci OŘ.

Předpokládá se, že samotná konfigurace bude z větší části v pravomoci Správy železnic, organizační složky CTD. Zhotovitel ve spolupráci s CTD a O14 stanoví technologický postup a časový harmonogram nasazení a implementace v jednotlivých OŘ.

## 6 Ochrana elektrických rozvodů

### 6.1 Prostředí

Vnitřní prvky sdělovacího zařízení jsou umístěny uvnitř budov v prostředí normálním dle ČSN 33 2000-3. Vnější kabely a prvky jsou konstruované pro vnější prostředí.

### 6.2 Ochrana před nebezpečným dotykem živých částí

U živých částí ve sdělovacích místnostech bude ochrana před nebezpečným dotykem živých částí provedena zábranou, neboť se jedná o umístění zařízení v prostorách přístupných pouze určeným pracovníkům s elektrotechnickou kvalifikací ve smyslu čl. 4212.3N3 ČSN 33 2000-4-41 a čl. 5.4 ČSN 34 2600. Dveře musí být uzamčeny a opatřeny bezpečnostními tabulkami podle ČSN 34 2600.

### 6.3 Ochrana před nebezpečným dotykem neživých částí

Pro ochranu před nebezpečným dotykem neživých částí platí příslušná ustanovení ČSN 34 2600 a ČSN 33 2000-4-41. Podle druhu jednotlivých napájecích soustav se užívá následujících způsobů ochrany:

- Ochrana samočinným odpojením od zdroje v síti TNC-S 3x400/230V, 50Hz (3x380/220V)
- Ochrana neživých částí obvodů FELV (napájení malým stejnosměrným napětím 24V, 48V, 60V).

Ochrana neživých částí obvodů FELV (napájení malým stejnosměrným napětím 24V, 40V, 48V, 60V) tím, že se propojí tyto neživé části s ochrannou soustavou sítě IT (tzn. s ochranným uzemněním neživých částí sítě IT). Pokud by dodavatel doložil, že zdroje malého stejnosměrného napětí i ostatní prvky v těchto obvodech (jako relé, stykače apod.) a uspořádání obvodů splňují požadavky, které jsou kladeny na obvody SELV podle čl.411.1.2 ČSN 33 2000-4-41, pak by se tyto obvody považovaly za obvody SELV a splňovaly by ochranu jak neživých, tak i živých částí.

U zařízení v prostorách normálních a nebezpečných stačí provést ochranu základní, u zařízení umístěného v prostorách zvlášť nebezpečných se provede s ohledem na prostředí ochrana zvýšená tím, že se provede doplňkové pospojování neživých částí. Tato doplňková ochrana je dovolena v kombinaci s ochranou samočinným odpojením v síti IT.

## **7 Životní prostředí, likvidace odpadů**

Hospodaření s odpady během výstavby a při vlastním provozu se bude řídit ustanovením zákona č. 2185/2001Sb. o odpadech a dalšími předpisy v odpadovém hospodářství.

Likvidace odpadů je prováděna podle programu odpadového hospodářství viz Vyhláška MŽP č. 383/2001Sb. o podrobnostech nakládání s odpady. Odpadový materiál bude uložen dle kategorizace odpadů nezávadným způsobem na řízenou skládku, kde musí dodavatel uzavřít smlouvu o uložení odpadového materiálu s osobou oprávněnou k nakládání s odpady.

## 8 Bezpečnost a ochrana zdraví při práci

Práce na zabezpečovacím zařízení a vedení podle této DUR mohou řídit a provádět pouze pracovníci s předepsanou kvalifikací (vzdělání, odborná praxe, školení, přezkoušení atd.) a zdravotní způsobilostí.

Při práci je třeba dodržovat stanovené technologické postupy a platné technické i bezpečnostní předpisy. Týká se to především ohrožení vyplývajících z práce na elektrických zařízeních, práce v kolejišti a souběhu prací na různých PS a SO stavby.

Pracoviště musí být předepsaným způsobem vybaveno a zajištěno.

Kromě obecných kvalifikačních předpokladů (odborné vzdělání a praxe v přísl. profesní specializaci) je třeba respektovat předpisy:

- SŽDC Zam1 Předpis o odborné způsobilosti a znalosti osob při provozování dráhy a drážní dopravy
- SŽDC Bp1 – Předpis o bezpečnosti a ochraně zdraví při práci

Příslušné normy TNŽ a elektrotechnické normy ČSN zejména pak:

- ČSN 33 2000-4-41 – Elektrotechnické předpisy ČSN. Všeobecné přepisy pro ochranu před nebezpečným dotykovým proudem
- ČSN 33 2160 – Elektrotechnické předpisy. Předpisy pro ochranu sdělovacích vedení a zařízení před nebezpečnými vlivy trojfázových vedení VN, VVN, ZVN
- ČSN 34 2040 – Elektrotechnické předpisy ČSN. Předpisy pro ochranu sdělovacích a zabezpečovacích vedení a zařízení před nebezpečnými a rušivými vlivy elektrické trakce 25 kV, 50 Hz
- ČSN 34 2300 – Předpisy pro vnitřní rozvody sdělovacích vedení

## 9 Pokyny pro montáž a demontáž

Veškeré práce spojené s montáží a demontáží zabezpečovacího zařízení a kabelů (optické, metalické) jsou obvyklé a nevyžadují zvláštního upozornění. Je třeba postupovat tak, aby demontovaná zařízení byla i nadále použitelná pro další možnou montáž do nových lokalit nebo popř. na náhradní díly.

### 9.1 Požadavky na zabezpečení provozu a realizace

Před započítím prací bude bezpodmínečně nutné pro pracovní postupy zkoordinovat návaznosti a styčné body tohoto PS s navazujícími PS a SO, a tím zajistit proveditelnost navrženého technického řešení.

Pro provedení tohoto PS bude nutná stavební připravenost zařízení, zajištění přístupnosti ze strany provozovatele, zajištění výluky a náhradního napájení, zajištění dopravy strojů a el. zař. Realizační firma měla oprávnění pro práci na zařízení Správy železnic dle předpisu SŽDC Zam 1.

### 9.2 Péče o životní prostředí

Při navrhované výstavbě je třeba dodržovat z hlediska péče o životní prostředí především tato všeobecně platná opatření:

- Mechanismy používané při provádění zemních prací musí být správně seřizeny (exhalace!) a běh motorů musí být omezen na nezbytně nutnou dobu (zemní práce, chránička).
- Ekologicky nebezpečný odpad (např. zbytky barev, laků, rozpouštědel, ředidel, ropných produktů, elektrolytu, odřezky kabelů a jejich obalů atd.) musí být odborně likvidován podle ekologických a bezpečnostních zásad – nikdy nesmí být ponechán na místech prací.
- Po dokončení prací musí být staveniště řádně uklizeno. To platí zejména pro úseky kabelové rýhy prováděné v závěrečných fázích stavby (např. nástupiště), kde je nutné odklidit přebytečnou zeminu a uvést povrch do stavu umožňujícího finální úpravu povrchu
- Předpokládané nároky na likvidaci odpadových materiálů jsou u tohoto provozního souboru minimální, zejména proto, že nebudou prováděny žádné demoliční práce. Zbytky kabelů a vodičů, stavebních nátěrů, nátěrových hmot a ředidel jakož i komunální odpad budou likvidovány jednotlivými postupy v rámci stavby.